JPA01-209561

⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平1-209561

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　平成1年(1989)8月23日
G 06 F 15/00		7361-5B	
9/06	330	B-7361-5B	
12/14	310	Z-7737-5B	審査請求　未請求　請求項の数 1　(全4頁)

㊹発明の名称　セキュリテイ管理処理方式

㉑特　願　昭63-34341
㉒出　願　昭63(1988)2月17日

㉒発明者　末成　徹　神奈川県川崎市中原区上小田中1015番地　富士通株式会社内
㉑出願人　富士通株式会社　神奈川県川崎市中原区上小田中1015番地
㉔代理人　弁理士　井桁　貞一

明細書

1　発明の名称

セキュリティ管理処理方式

2　特許請求の範囲

複数の利用者に共用可能な資源を有する計算機システムにおいて、

所要の各業務ごとに、業務識別名、許可利用者識別名、及び該共用可能な資源のうちの所要資源の資源識別名を指定する許可リスト(12)と、

該利用者が利用者識別名及び許可識別名を入力した場合に、該許可識別名に対応する該許可リストを検索する手段(11)と、

該検索した許可リストに指定された該許可利用者識別名に、該入力した利用者識別名が指定されていることを条件として、該許可リスト(12)に指定された該業務識別名によって定まる業務の実行を開始させる手段(11、13)と、

該業務の実行中に使用する資源を、該許可リスト(12)に指定されている該資源識別名の範囲に限定する手段(13)とを設けたことを特徴とするセキュリティ管理処理方式。

3　発明の詳細な説明

(概　要)

複数の利用者に共用される資源を有する計算機システムのセキュリティ管理に関し、

業務を実行する利用者及びその業務で使用可能な資源を業務オリエンテッドに管理することの容易なセキュリティ管理処理方式を目的とし、

複数の利用者に共用可能な資源を有する計算機システムにおいて、所要の各業務ごとに、業務識別名、許可利用者識別名、及び該共用可能な資源のうちの所要資源の資源識別名を指定する許可リストと、該利用者が利用者識別名及び許可識別名を入力した場合に、該許可識別名に対応する該許可リストを検索する手段と、該検索した許可リストに指定された該許可利用者識別名に、該入力した利用者識別名が指定されていることを条件として、該許可リストに指定された該業務識別名に

よって定まる業務の実行を開始させる手段と、該業務の実行中に使用する資源を、該許可リストに指定されている該資源識別名の範囲に限定する手段とを設けるように構成する。

〔産業上の利用分野〕

本発明は、複数の利用者に共用される資源を有する計算機システムのセキュリティ管理、特に業務を実行する利用者及びその業務で使用可能な資源を業務オリエンテッドに管理するようにしたセキュリティ管理処理方式に関する。

複数の利用者が共用する計算機システムにおいては、プログラム、データ等の共用可能な資源について、データ内容の秘密保持、不当な改竄の防止等のいわゆるセキュリティ維持のための管理が一般に必要とされる。

〔従来の技術〕

第2図は計算機システムの構成例を示すブロック図である。

計算機システムの利用者は、処理装置1に接続した端末2から所要の指令等を入力して、記憶装置3に格納されたプログラムファイル4から業務に必要なプログラムを指定して実行することにより、記憶装置3に格納されたデータファイル5の所要データ或いは端末2から入力するデータ等を処理して、ファイルを更新し、又必要な処理結果を端末2に出力させる。

このようなシステムでセキュリティ管理を行う場合には、例えば先ず利用者が端末2からシステムにアクセスしたとき、セキュリティ制御部6が利用者識別名と利用者パスワードの入力を求め、両入力の対応を利用者管理リスト7によって確認できた場合のみ、業務の処理の開始を許し、利用者識別名と利用者パスワードが対応しない場合にはシステムへのアクセスを拒絶し、このようにして利用者がシステムの利用者管理リスト7に予め登録されている利用者であることを確認する。

次に利用者が、業務のために所要のプログラムを稼働し、必要なデータファイルにアクセスするために、それらのファイル名を指定してアクセスを要求した場合に、それらのファイがセキュリティ管理の必要なファイルであると、セキュリティ制御部6はそれぞれについてファイルパスワードの入力を要求する。

セキュリティ制御部6は利用者が入力した各ファイルパスワードを、ファイル管理リスト8によって各ファイル名に対応するかチェックし、ファイル名に対応する正しいファイルパスワードが入力された場合のみ、そのファイルへのアクセスを許し、このようにして、システムに登録された正当な利用者が、ファイルパスワードを知らされているファイルにのみアクセスできるように管理することができる。

〔発明が解決しようとする課題〕

前記のようなセキュリティ管理の処理方式は、各利用者が個別に利用するような計算センタ等に向いていて、管理の融通性はあるが、セキュリティ管理を細かく行おうとすると利用者に煩雑な操作を要求するようになる等の問題がある。

特に、近年増加しているような例えば中型の計算機システムを一事務所内の多数の要員が共用して、比較的広い範囲の業務に使用するような場合には、利用者に要求する操作が簡単で適切なセキュリティ管理の可能な方式が望まれる。

本発明は、各利用者が計算機を使用して実行する業務を基本にして、業務を実行する利用者及びその業務で使用可能な資源を業務オリエンテッドに管理することの容易なセキュリティ管理処理方式を目的とする。

〔課題を解決するための手段〕

第1図は、本発明の構成を示すブロック図である。

図は計算機システムの構成を示し、処理装置10の11はシステムにアクセスする利用者の指定する業務の実行可否を、記憶装置15に格納する許可リスト12を検索して決定するアクセス制御部、13は業務の実行中に、その業務に対応する許可リスト

12a によって、資源の使用を監視制御する実行制御部である。

〔作　用〕

許可リスト12には、所要の各業務ごとに業務識別名、許可利用者識別名、及び共用可能な計算機資源のうちの所要の資源の資源識別名をそれぞれ指定する。

利用者がある業務を実行する場合には、端末2から利用者識別名及び許可識別名を入力し、アクセス制御部11が、入力された許可識別名に対応する該許可リストを検索し、入力された利用者識別名が、その許可リストに許可利用者識別名として指定されているかチェックして、該当の許可利用者識別名があれば、業務を開始させるためにその許可リストの内容を許可リスト12a として実行制御部13に渡す。

実行制御部13は、その許可リストに指定された業務識別名によって定まる業務の実行を開始させ、又業務の実行中に使用する資源を、その許可リスト12a に指定されている資源識別名の範囲に限定するように制御する。

以上の処理方式により、利用者は常にシステムにアクセスする場合に、自身の利用者識別名の他には、必要な各業務に対する許可識別名のみを知っていればよく、システムでは業務ごとの許可リストにより、セキュリティを維持するに必要なだけ使用資源の限定等を行うことができる。

〔実施例〕

本発明によるセキュリティ管理を適用する計算機システムでは、原則として各利用者ごとに利用者識別名を定める。又セキュリティ管理を考慮して分類した、セキュリティ管理の必要な業務ごとに1個以上の許可識別名を設け、それらの各業務に対応して許可リスト12を設定しておく。

それらの利用者識別名及び許可識別名は原則として公開せず、必要な利用者のみに知らせておくように運用するものとする。

各許可リスト12には、各業務ごとの業務識別名、その業務の実行を許可される利用者を示す1以上の利用者識別名からなる許可利用者識別名、及び共用可能な計算機資源のうちの所要の資源の資源識別名をそれぞれ設定する。

こゝで問題とする計算機の資源には、例えばデータのファイル、プログラム又はコマンド（コマンドを実行するプログラム）等があり、それぞれファイル名、コマンド名、ファイルの集合であるライブラリを指定するライブラリ名等によってプログラムファイル4、データファイル5等の特定のファイルを指定することにより、許可リスト12に指定されている資源のみの使用を許可するように制御する。

利用者が或る業務を実行する場合には、端末2から利用者識別名及び許可識別名を入力する。

アクセス制御部11がその入力を受け取り、入力された許可識別名に対応する該許可リストを検索する。そのために例えばアクセス制御部11は許可識別名と許可リストの格納アドレスとの対応表を保持して、対応表から所要の許可識別名を走査する。

該当の許可リストがあれば、入力された利用者識別名が、その許可リスト12に、許可利用者識別名として指定されているかチェックし、許可されていれば業務を開始させるためにその許可リストの内容を許可リスト12a として実行制御部13に渡す。又、該当の許可リストが無いか、該当の許可利用者識別名が無ければ、利用者に対してアクセスを拒絶する。

実行制御部13は、その許可リスト12a に指定された業務識別名によって定まる業務の実行を開始させる。この業務開始は、例えば業務識別名をジョブ名として登録されているジョブ制御情報を使用することにより、通常の手順で行うことができる。

業務が開始されると実行制御部13は、実行中の業務を監視するために、業務中で新たな資源の要求が発生するごとに制御を渡され、要求の資源を、許可リスト12a に指定されている資源識別名を参照してチェックし、許可されていれば制御を返し

て、業務の処理を進める。許可されていない資源が要求された場合には、例えばその業務の実行を中断させる等の処理を行う。

〔発明の効果〕

以上の説明から明らかなように本発明によれば、複数の利用者の共用資源を有する計算機システムにおいて、業務を実行する利用者及びその業務で使用可能な資源を業務オリエンテッドに管理して、利用者には業務を指定する許可識別名を提示させるのみで、業務ごとに必要なレベルのセキュリティ管理を行うことができるので、計算機システムのセキュリティと利用性を向上するという著しい工業的効果がある。

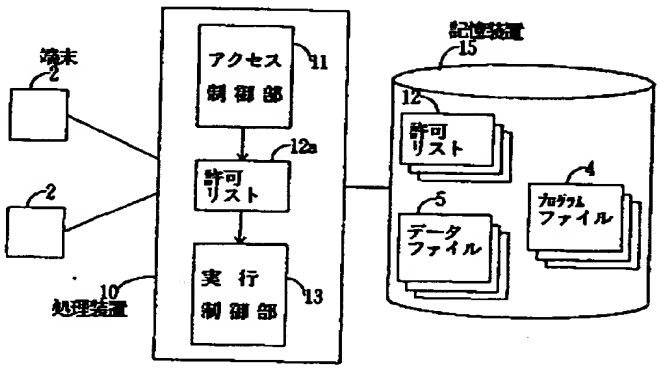
4　図面の簡単な説明

第1図は本発明の構成を示すブロック図、
第2図は従来の構成例を示すブロック図
である。

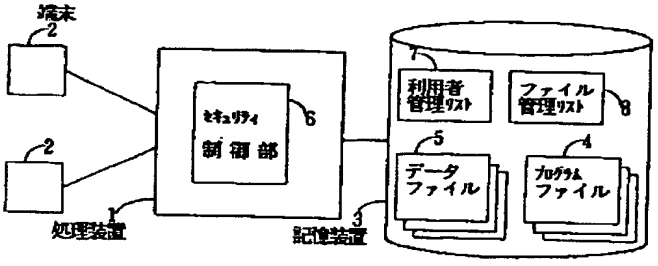
図において、

1、10は処理装置、　2は端末、
3、15は記憶装置、　4はプログラムファイル、
5はデータファイル、　6はセキュリティ制御部、
7は利用者管理リスト、
8はファイル管理リスト、
11はアクセス制御部、　12、12a は許可リスト、
13は実行制御部
を示す。

代理人　弁理士　井桁　貞一



本発明の構成を示すブロック図
第　1　図



従来の構成例を示すブロック図
第　2　図